S&H Form: FORM PTO-1390 (2/01)

U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER
1454.1203

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/DE00/01788	May 31, 2000	June 15, 1999

10/009975

TITLE OF INVENTION
METHOD AND SYSTEM FOR VERIFYING THE AUTHENTICITY OF A FIRST COMMUNICATION PARTICIPANTS IN A COMMUNICATIONS NETWORK

APPLICANT(S) FOR DO/EO/US
Günther HORN et al.

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a FIRST submission of items concerning a filing under 35 U.S.C. 371.
2. ☒ This is an express request to immediately begin national examination procedures (35 U.S.C. 371(f)).
3. ☒ The US has been elected by the expiration of 19 months from the priority date (PCT Article 31).
4. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
   a. ☒ is transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ has been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US).
5. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
6. ☐ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
   a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
   b. ☐ have been transmitted by the International Bureau.
   c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
7. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
8. ☐ An oath or declaration of the inventor (35 U.S.C. 371(c)(4)).
9. ☒ A translation of the Annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 10-15 below concern document(s) or information included:

10. ☐ An Information Disclosure Statement Under 37 CFR 1.97 and 1.98.
11. ☐ An assignment document for recording.
    Please mail the recorded assignment document to:
    a. ☐ the person whose signature, name & address appears at the bottom of this document.
    b. ☐ the following:
12. ☒ A preliminary amendment.
13. ☒ A substitute specification
14. ☐ A change of power of attorney and/or address letter.
15. ☒ Other items or information: First page of published International Application; Preliminary Examination Report; International Search Report; Letter to the Examiner Requesting Approval of Changes to the Drawings.

10/009975 JC07 Rec'd PCT/PTO 17 DEC 2001

☒ The U.S. National Fee (35 U.S.C. 371(c)(1)) and other fees as follows:

CLAIMS	(1) FOR	(2) NUMBER FILED	(3) NUMBER EXTRA	(4) RATE	(5) CALCULATIONS
	TOTAL CLAIMS	19 -20=	10	x $ 18.00	0.00
	INDEPENDENT CLAIMS	2 -3=	0	x $ 84.00	0.00
	MULTIPLE DEPENDENT CLAIM(S) (if applicable)			+$280.00	0.00
	BASIC NATIONAL FEE (37 CFR 1.492(a)(1)-(4): ☐ Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO .....$1,040 ☒ International preliminary examination fee (37 C.F.R. 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO.....$ 890 ☐ International preliminary examination fee (37 C.F.R. 1.482) not paid to USPTO but international search fee (37 C.F.R. 1.445(a)(2) paid to USPTO...$ 740 ☐ International preliminary examination fee paid to USPTO (37 CFR 1.482) but all claims did not satisfy provision of PCT Article 33(1)-(4).....$ 710 ☐ International preliminary examination fee paid to USPTO (37 CFR 1.482) and all claims satisfied provisions of PCT Article 33(2) to (4) .....$ 100				890.00
	Surcharge of $130 for furnishing the National fee or oath or declaration later than ☐ 20 ☐ 30 mos. from the earliest claimed priority date (37 CFR 1.482(e)).				0.00
			TOTAL OF ABOVE CALCULATIONS		890.00
	Reduction by 1/2 for filing by small entity, if applicable. Affidavit must be filed also. (Note 37 CFR 1.9, 1.27, 1.28.)				
			SUBTOTAL		890.00
	Processing fee of $130 for furnishing the English Translation later than [ ] 20 [ ] 30 mos. from the earliest claimed priority date (37 CFR 1.482(f)).				
			TOTAL NATIONAL FEE		890.00
	Fee for recording the enclosed assignment (37 CFR 1.21(h)).				+
			TOTAL FEES ENCLOSED		890.00

a. ☒ A check in the amount of $890.00 to cover the above fees is enclosed.
b. ☐ Please charge my Deposit Account No. 19-3935 in the Amount of $ to cover the above fees. A duplicate copy of this sheet is enclosed.
c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 19-3935. A duplicate copy of this sheet is enclosed.

21171
PATENT TRADEMARK OFFICE

SUBMITTED BY: STAAS & HALSEY LLP

Type Name	Mark J. Henry	Reg. No.	36,162
Signature	Mark J. Henry	Date	Dec. 17, 2001

4/PRTS

Docket No.: 1454.1203

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

PCT National Phase of PCT/DE00/01788

Günther HORN et al.

Serial No. Group Art Unit: To be assigned

Confirmation No.

Filed: Examiner: To be assigned

For: METHOD AND SYSTEM FOR VERIFYING THE AUTHENTICITY OF A FIRST COMMUNICATION PARTICIPANTS IN A COMMUNICATIONS NETWORK

LETTER TO THE EXAMINER REQUESTING APPROVAL OF THE CHANGES TO THE DRAWINGS

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

It is respectfully requested that the Examiner having jurisdiction over the subject application approve the amendments to the drawings as indicated in RED on the attached copy of Figures 1, 2 and 4.

Respectfully submitted,

STAAS & HALSEY LLP

Date: Dec. 17, 2001

By: Mark J. Henry
Registration No. 36,162

700 Eleventh Street, NW, Suite 500
Washington, D.C. 20001
(202) 434-1500

FIG 1

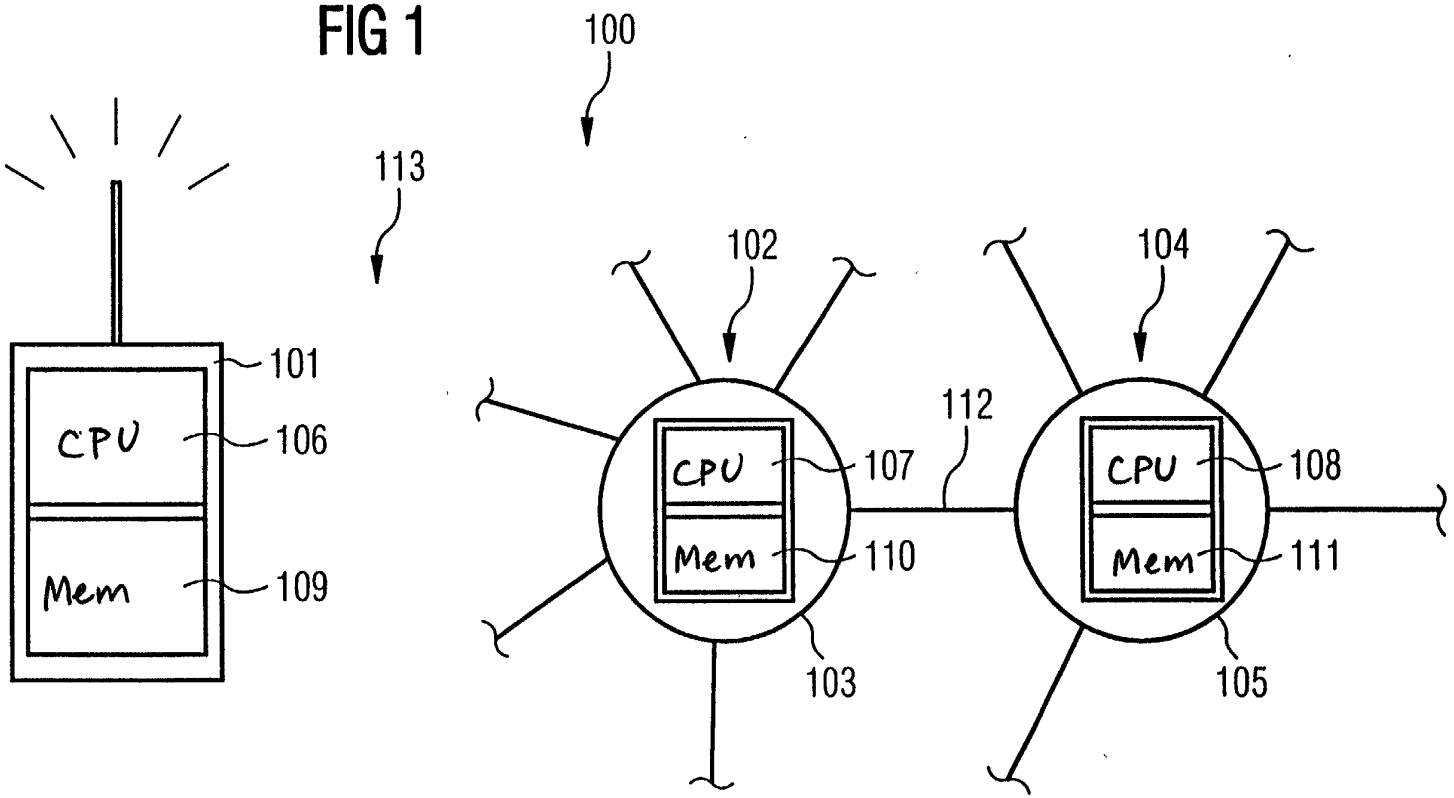


FIG 2

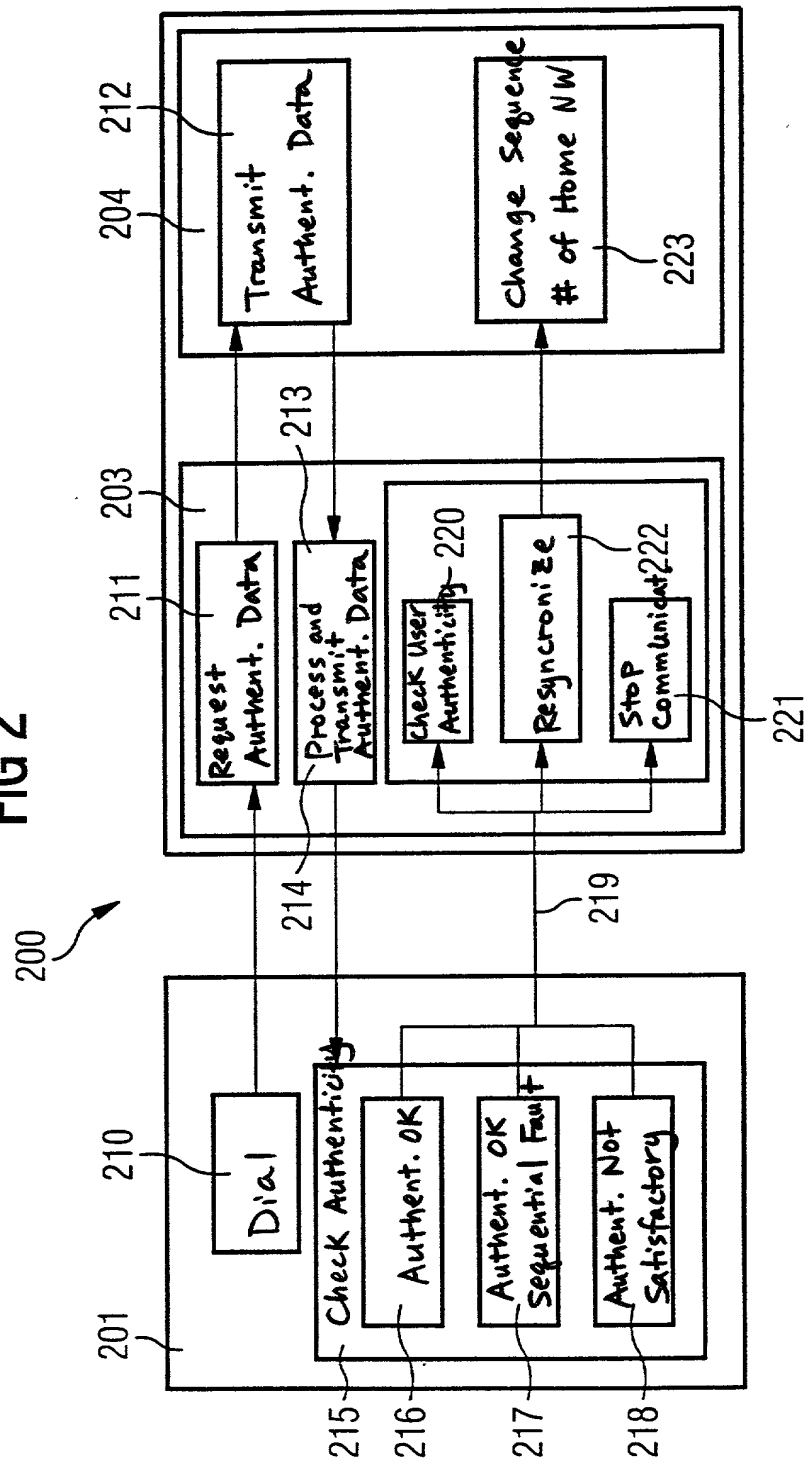
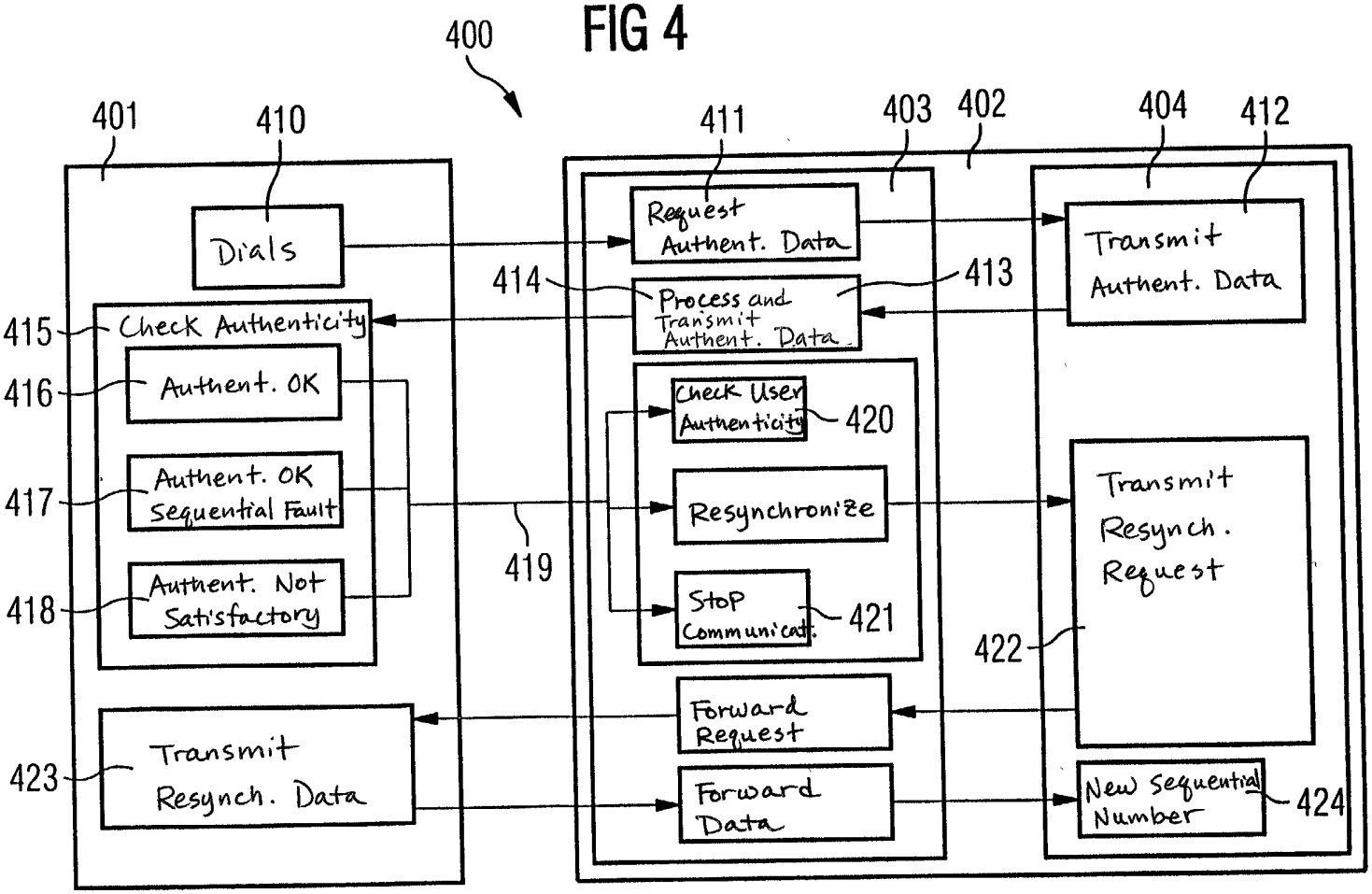


FIG 4



Docket No.: 1454.1203

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:

PCT National Phase of PCT/DE00/01788

Günther HORN et al.

Serial No. Group Art Unit: To be assigned

Confirmation No.

Filed: Examiner: To be assigned

For: METHOD AND SYSTEM FOR VERIFYING THE AUTHENTICITY OF A FIRST COMMUNICATION PARTICIPANTS IN A COMMUNICATIONS NETWORK

PRELIMINARY AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Before examination of the above-identified application, please amend the application as follows:

IN THE SPECIFICATION:

Please REPLACE the specification originally filed with the enclosed Substitute Specification.

IN THE CLAIMS:

Please CANCEL claims 1-11.

Please ADD new claims 12-30 in accordance with the following:

12. (NEW) A method for checking the authenticity of a first communication subscriber in a communications network, comprising:

forming a first fault information item in the first communication subscriber using a fault detection data item of the first communication subscriber and an information item relating to a

random data item which has been transmitted to the first communication subscriber by a second communication subscriber in the communications network;

transmitting the first fault information to the second communication subscriber by the first communication subscriber,

forming a second fault information item in the second communication subscriber using a fault detection data item of the second communication subscriber and the information item relating to the random data item;

checking the authenticity of the first communication subscriber in the second communication subscriber using the first fault information item and the second fault information item.

13. (NEW) The method as claimed in claim 12, wherein a difference is determined between the fault detection data item of the first communication subscriber and the fault detection data item of the second communication subscriber.

14. (NEW) The method as claimed in claim 13, wherein the difference is limited.

15. (NEW) The method as claimed in claim 12, wherein the first and second communication subscribers are part of a mobile phone system.

16. (NEW) The method as claimed in claim 13, wherein the first and second communication subscribers are part of a mobile phone system.

17. (NEW) The method as claimed in claim 14, wherein the first and second communication subscribers are part of a mobile phone system.

18. (NEW) A system for checking authenticity in a communications network, comprising:

a first communication subscriber to form a first fault information using a fault detection data item of the first communication subscriber and an information item relating to a random data item which has been transmitted to the first communication subscriber, and to transmit the first fault information;

a second communication subscriber to transmit the information relating to the random data item to the first communication subscriber, to receive the first fault information

from the first communication subscriber, to form a second fault information using a fault detection data item of the second communication subscriber and the information relating to the random data item, and to check the authenticity of the first communication subscriber using the first fault information and the second fault information.

19. (NEW) The system as claimed in claim 18, wherein the first communication subscriber is a service provider and the second communication subscriber is a service user in the communications network.

20. (NEW) The system as claimed in claim 19, wherein the service provider is a mobile phone operator and the service user is a mobile phone.

21. (NEW) The system as claimed in claim 18, wherein the fault detection data items are sequential numbers.

22 . (NEW) The system as claimed in claim 21, wherein the information relating to the random data item is a random number.

23 . (NEW) The system as claimed in claim 18, wherein the first and second communication subscribers are part of a mobile phone system.

24. (NEW) The system as claimed in claim 21, wherein the first communication subscriber is a service provider and the second communication subscriber is a service user in the communications network.

25. (NEW) The system as claimed in claim 24, wherein the service provider is a mobile phone operator and the service user is a mobile phone.

26. (NEW) The system as claimed in claim 22, wherein the first communication subscriber is a service provider and the second communication subscriber is a service user in the communications network.

27. (NEW) The system as claimed in claim 26, wherein the service provider is a mobile phone operator and the service user is a mobile phone.

28. (NEW) The system as claimed in claim 19, wherein the fault detection data items are sequential numbers.

29. (NEW) The system as claimed in claim 28, wherein the information relating to the random data item is a random number.

30. (NEW) The system as claimed in claim 29, wherein the service provider is a mobile phone operator and the service user is a mobile phone.

REMARKS

This Preliminary Amendment is submitted to improve the form of the specification as originally-filed. A substitute specification and marked-up copy of the original specification are enclosed. No new matter is added to these documents.

It is respectfully requested that this Preliminary Amendment be entered in the above-referenced application.

If any further fees are required in connection with the filing of this Preliminary Amendment, please charge same to our Deposit Account No. 19-3935.

Respectfully submitted,

STAAS & HALSEY LLP

Date: Dec. 17, 2001

By: [signature]
Mark J. Henry
Registration No. 36,162

700 Eleventh Street, NW, Suite 500
Washington, D.C. 20001
(202) 434-1500

SUBSTITUTE SPECIFICATION

TITLE OF THE INVENTION

METHOD AND SYSTEM FOR VERYFYING THE AUTHENTICITY OF A FIRST COMMUNICATION PARTICIPANTS IN A COMMUNICATIONS NETWORK

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is based on and hereby claims priority to German Application No. 19927 271.9 filed on June 15, 1999 in Germany, and PCT Application No. PCT/DE00/01788 filed on May 31, 2000, the contents of which are hereby incorporated by reference.

BACKGROUND OF THE INVENTION

[0002] The invention relates to a method and an arrangement for checking the authenticity of a first communication subscriber in a communications network.

[0003] In a communications network, data is generally transmitted between communication subscribers, for example a service provider and a service user. In order to protect a communications network against penetration of an unauthorized communication subscriber into the communications network, the authenticity of each communication subscriber is generally checked.

[0004] 3G TS 33.102 Version 3.0.0 Draft Standard, 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Security Architecture, 05/1999 ("the 3G reference") discloses a method and an arrangement for checking the authenticity of a communication subscriber, in particular of a service provider or of a service user in a communications network.

[0005] The method known from the 3G reference and the corresponding arrangement are based on what is referred to as 3G TS 33.102 Version 3.0.0 Draft Standard, which describes a security architecture of a mobile phone system.

[0006] In Fig. 4, the procedure during the checking of the authenticity of a communication subcriber, such as is known from the 3G reference is illustrated symbolically and parts thereof will be explained below briefly.

[0007] A transmission of data is illustrated in Fig. 4 by an arrow in each case. A direction of an arrow characterizes a transmission direction during a data transmission.

[0008] Fig. 4 shows a mobile phone system 400, comprising a user 401 of a communication service, for example a mobile phone, and a provider 402 of a communication service. The provider 402 comprises a dial-in network 403 with a dial-in network operator from which the user 401 locally requests a communication service, and a home network 404 with a home network operator with which the user 401 is signed on and registered.

[0009] In addition, the user 401, the dial-in network 403 and the home network 404 each have a central processing unit with a memory, for example a server (central computing unit), with which processing unit the procedure described below is monitored and controlled and on which memory data is stored.

[0010] The dial-in network 403 and the home network 404 are connected to one another via a data line over which digital data can be transmitted. The user 401 and the dial-in network 403 are connected to one another via any desired transmission medium for the transmission of digital data.

[0011] During a communication, the user 401 dials 410 into the dial-in network 403. At the start of the communication, checking of both the authenticity of the user 401 and the authenticity of the provider 402 is carried out.

[0012] To do this, the dial-in network 403 requests 411 what is referred to as authentication data from the home network 404, with which data the authenticity of the user 401 and of the provider 402 can be checked.

[0013] The authentication data which is obtained from the home network 404 comprises a random number and a sequential number of the provider 402. The sequential number of the provider 402 is obtained in such a way that a counter of the provider 402 increases the sequential number of the provider 402 by the value 1 at each attempt at communication between the user 401 and the provider 402.

[0014] It is to be noted that the random number and the sequential number of the provider 402 only constitute part of the authentication data and are not to be understood as comprehensive. Further authentication data is known from the 3G reference.

[0015] The home network 404 transmits 412 the requested authentication data to the dial-in network 403. The dial-in network 403 processes the received authentication data in a suitable way 413, and transmits the processed authentication data to the user 401.

[0016] The user 401 checks 415 the authenticity of the provider 402 using a dedicated sequential number, which is handled in a way corresponding to the sequential number of the provider 402, and using the sequential number of the provider 402.

[0017] The procedure during the checking of the authenticity of the provider 402 is described in the 3G reference.

[0018] A result of the checking of the authenticity of provider 402, "authenticity of provider satisfactory" 416, "authenticity of provider satisfactory but sequential fault has occurred" 417 or "authenticity of provider not satisfactory" 418, is transmitted 419 from the user 401 to the provider 402.

[0019] In the case of the result "authenticity of provider satisfactory" 416, the dial-in network 403 checks 420 the authenticity of the user 401 as described in the 3G reference.

[0020] In the case of the result "authenticity of provider not satisfactory" 418, the communication is interrupted and/or restarted 421.

[0021] In the case of the result "authenticity of provider satisfactory but a sequential fault has occurred" 417, resynchronization takes place in such a way that the home network 404 transmits 422 a resynchronization request to the user 401. The user responds with a resynchronization response in which resynchronization data is transmitted 423 to the home network 404. The sequential number of the provider 402 is changed 424 as a function of the resynchronization response. The authenticity of the user 401 is then checked, as is known from the 3G reference.

[0022] The procedure described has the disadvantage that during checking of the authenticity of a communication subscriber, in particular during the checking of the authenticity of a service provider, a large amount of data has to be transmitted between the communication subscribers.

SUMMARY OF THE INVENTION

[0023] One aspect of the invention is thus based on simplifying and improving the known method and the known arrangement, to yield a simplified and improved arrangement for checking the authenticity of a communication subscriber in a communications network.

[0024] In the method for checking the authenticity of a first communication subscriber in a communications network, a first fault information item is formed in the first communication subscriber using a fault detection data item of the first communication subscriber and an information item relating to a random data item. In a second communication subscriber in the communications network, a second fault information item is formed using a fault detection data item of the first communication subscriber and the information relating to the random data item.

[0025] The authenticity of the first communication subscriber is checked using the first fault information item and the second fault information item.

[0026] In the arrangement for checking the authenticity of a first communication subscriber in a communications network, the first communication subscriber is set up in such a way that a first fault information item can be formed using a fault detection data item of the first communication subscriber and an information item relating to a random data item. In addition, the arrangement has a second communication subscriber in the communications network which is set up in such a way that a second fault information item can be formed using a fault detection data item of the second communication subscriber and the information relating to the random data item. The authenticity of the first communication subscriber can be checked using the first fault information item and the second fault information item.

[0027] The checking of the authenticity of a communication subscriber in a communications network is to be understood as meaning method steps which are carried out in the wider sense with checking of the authorization of a communication subscriber for access to a communications network or participation in communication in a communications network.

[0028] This thus encompasses both method steps which are carried out within the scope of the checking of the authorization of a communication subscriber for access to a communications network and such method steps which are carried out within the scope of the processing or the administration of data which is used in the checking.

[0029] The developments described below relate to the method and to the arrangement.

[0030] The development described below can be implemented either using software or hardware, for example using a specific electrical circuit.

[0031] In one refinement, the first communication subscriber is a service provider and/or the second communication subscriber is a service user in the communications network.

[0032] A sequential number is preferably used as the fault detection data item.

[0033] In one refinement, the information relating to the random data item is a random number.

[0034] In one development, the checking of the authenticity is simplified by determining a difference between the fault detection data item of the first communication subscriber and the fault detection data item of the second communication subscriber.

[0035] In one refinement, the checking of the authenticity is further improved with respect to the security of the communications network by limiting the difference.

[0036] One development is preferably used within the scope of a mobile phone system. In the mobile phone system, the service user is implemented as a mobile phone and/or the service provider is implemented as a mobile phone network operator.

BRIEF DESCRIPTION OF THE DRAWINGS

[0037] These and other objects and advantages of the present invention will become more apparent and more readily appreciated from the following description of the preferred embodiments, taken in conjunction with the accompanying drawings of which:

Fig. 1 shows a mobile phone system;

Fig. 2 shows an outline in which checking of the authenticity of a communication

subscriber is illustrated symbolically;

Fig. 3 shows a flowchart in which individual method steps are illustrated during checking of the authenticity of a service provider in a communications network; and

Fig. 4 shows an outline in which checking of the authenticity of a communication subscriber in accordance with the 3G TS 33.102 Version 3.0.0 Standard is illustrated symbolically.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0038] Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings, wherein like reference numerals refer to like elements throughout.

Exemplary embodiment: mobile phone system

[0039] A mobile phone system 100 is illustrated in Fig. 1. The mobile phone system 100 comprises a mobile phone 101, a local dial-in network 102 with a dial-in network operator 103 and a home network 104 with a home network operator 105.

[0040] The mobile phone 101 is signed on and registered in the home network 104.

[0041] In addition, the mobile phone 101, the dial-in network 102 and the home network 104 each have a central processing unit 106, 107, 108 with a memory 109, 110, 111, with which processing units 106, 107, 108 the procedure described below is monitored and controlled, and on which memories 109, 110, 111 data is stored.

[0042] The dial-in network 102 and the home network 104 are connected to one another via a data line 112 via which digital data can be transmitted. The mobile phone 101 and the dial-in network 102 are connected to one another via any desired transmission medium 113 for transmitting digital data.

[0043] The procedure during the checking of the authenticity of the mobile phone 101 and the procedure during the checking of the authenticity of the home network 104 and/or of the home network operator 105 are illustrated symbolically in Fig. 2, and parts thereof will be explained below briefly.

[0044] The transmission of data in Fig. 2 is illustrated in each case by an arrow. A direction of an arrow characterizes a transmission direction during a data transmission.

[0045] The procedure which is described below and illustrated symbolically in Fig. 2 is based on what is referred to as a 3G TS 33.102 Version 3.0.0 Standard, which describes a security architecture of a mobile phone system and is described in the 3G reference.

[0046] During a communication, the mobile phone 201 dials 210 into the dial-in network 203. At the start of the communication, checking both of the authenticity of the mobile phone 201 and of the authenticity of the home network 204 and/or of the home network operator takes place.

[0047] To do this, the dial-in network 203 requests 211 authentication data from the home network 204, with which authentication data the authenticity of the user 201 and of the home network 204 and/or of the home network operator can be checked.

[0048] The authentication data which is determined by the home network 204 comprises a random number and a sequential number of the home network 204 (cf. Fig. 3 step 310). The sequential number of the home network 204 is determined in such a way that a counter of the home network 204 increases the sequential number of the home network 204 by the value 1 at each attempt at communication between the mobile phone 201 and the home network 204.

[0049] It is to be noted that the random number and the sequential number of the home network 204 only constitute part of the authentication data and are not to be understood as comprehensive. Further authentication data is specified in the 3G reference.

[0050] The home network 204 transmits 212 the requested authentication data to the dial-in network 203. The dial-in network 203 processes the received authentication data in a suitable way 213 and transmits the processed authentication data to the mobile phone 201.

[0051] The mobile phone 201 checks 215 the authenticity of the home network 204 using a dedicated sequential number which is handled in a way corresponding to the sequential number of the home network 204, and using the sequential number of the home network 204. In a way corresponding to the home network 204, the mobile phone 201 also has a counter.

[0052] The procedure during the checking of the authenticity of the home network 204 is described in the 3G reference. Method steps which differ therefrom are described below.

[0053] What is referred to as overflow checking of the counter of the mobile phone 201 is carried out within the scope of the checking of the authenticity of the home network 203. This overflow checking prevents overflowing of an acceptable numerical range of the counter of the mobile phone 201.

[0054] In the overflow checking, the following conditions are tested:

1) sequential number of the home network 204 > sequential number of the mobile phone 201;

2) sequential number of the home network 204 – sequential number of the mobile phone 201 < - predefinable deviation (1,000,000);

the following applying for the predefined deviation:

- predefinable deviation is sufficiently large in order to ensure, during normal or fault-free communications operation:

that the sequential number of the home network 204 – sequential number of the mobile phone 201 is not > predefinable deviation;

- the maximum permissable sequential number of the mobile phone 201/predefinable deviation is sufficiently large in order to ensure that the maximum permissible sequential number of the mobile phone 201 is not reached during operation.

[0055] The result of the checking of the authenticity of the home network 204, "authenticity satisfactory" 216, "authenticity satisfactory but a sequential fault has occurred" 217 or "authenticity not satisfactory" 218 is transmitted 219 to the home network 204 from the mobile phone 201.

[0056] In the case of the result "authenticity satisfactory" 216, the dial-in network 203 checks 220 the authenticity of the mobile phone 201, as described in 3G reference.

[0057] In the case of the result "authenticity not satisfactory" 218, the communication is interrupted or restarted 221.

[0058] In the case of the result "authenticity satisfactory but a sequential fault has occurred" 217, resynchronization 222 takes place. Resynchronization is to be understood as a change of the sequential number of the home network 204.

[0059] For this purpose, the mobile phone 201 transmits 222 resynchronization data to the dial-in network 203.

[0060] The resynchronization data comprises the same random number which was transmitted within the scope of the authentication data, and the sequential number of the mobile phone 201 (cf. Fig. 3 step 320).

[0061] The dial-in network 203 processes the resynchronization data in a suitable way and transmits the processed resynchronization data to the home network 204.

[0062] The home network 204 checks the sequential number of the mobile phone 201 and the sequential number of the home network 204 using the processed resynchronization data, and if appropriate changes 223 the sequential number of the home network 204 (cf. Fig. 3 step 330).

[0063] The home network 204 subsequently transmits new authentication data, which if appropriate comprises the changed sequential number of the home network 204, to the dial-in network 203.

[0064] In order to illustrate the described procedure, important steps 300 of the procedure are illustrated in Fig. 3.

[0065] Fig. 3 shows a first step 310 within the scope of which the authentication data (first fault information) is determined.

[0066] The resynchronization data (second fault information) is determined within the scope of a second step 320.

[0067] The sequential number of the mobile phone and the sequential number of the home network are checked within the scope of a third step 330, using the resynchronization data.

[0068] An alternative of the first exemplary embodiment is described below.

[0069] In the alternative exemplary embodiment, a method is implemented in which the home network is made more reliable with respect to a data loss in the event of a system crash.

[0070] For this purpose, the current sequential number of the home network is stored in the memory of the home network, in each case at a predefinable time interval. A sequential number of the home network which has been lost during a system crash of the home network is restored in such a way that a predefinable additional value is added to the value of the stored sequential number. The predefinable additional value is dimensioned in such a way that exceeding of the sum of the sequential number of the mobile phone and the predefinable deviation is not exceeded.

[0071] In the alternative exemplary embodiment, the predefinable additional value is determined in such a way that an average number of authentication attempts on one day by the home network, which number is determined during operation of the communications network, is multiplied by a factor with the value 10.

[0072] The invention has been described in detail with particular reference to preferred embodiments thereof and examples, but it will be understood that variations and modifications can be effected within the spirit and scope of the invention.

MARKED-UP COPY OF TRANSLATED INTERNATIONAL APPLICATION

[Description] TITLE OF THE INVENTION

METHOD AND [ARRANGEMENT]SYSTEM FOR [CHECKING]VERYFYING THE AUTHENTICITY OF A FIRST COMMUNICATION [SUBSCRIBER]PARTICIPANTS IN A COMMUNICATIONS NETWORK

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is based on and hereby claims priority to German Application No. 19927 271.9 filed on June 15, 1999 in Germany, and PCT Application No. PCT/DE00/01788 filed on May 31, 2000, the contents of which are hereby incorporated by reference.

BACKGROUND OF THE INVENTION

[0002] The invention relates to a method and an arrangement for checking the authenticity of a first communication subscriber in a communications network.

[0003] In a communications network, data is generally transmitted between communication subscribers, for example a service provider and a service user. In order to protect a communications network against penetration of an unauthorized communication subscriber into the communications network, the authenticity of each communication subscriber is generally checked.

[0004] [Document] 3G TS 33.102 Version 3.0.0 Draft Standard, 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Security Architecture, 05/1999 ("the 3G reference") discloses a method and an arrangement for checking the authenticity of a communication subscriber, in particular of a service provider or of a service user in a communications network.

[0005] The method known from [document (1)]the 3G reference and the corresponding arrangement are based on what is referred to as 3G TS 33.102 Version 3.0.0 Draft Standard, which describes a security architecture of a mobile phone system.

[0006] In Fig. 4, the procedure during the checking of the authenticity of a communication subcriber, such as is known from the [document(1)]3G reference is illustrated symbolically and parts thereof will be explained below briefly.

[0007] A transmission of data is illustrated in Fig. 4 by an arrow in each case. A direction of an arrow characterizes a transmission direction during a data transmission.

[0008] Fig. 4 shows a mobile phone system 400, comprising a user 401 of a communication service, for example a mobile phone, and a provider 402 of a communication service. The provider 402 comprises a dial-in network 403 with a dial-in network operator from which the user 401 locally requests a communication service, and a home network 404 with a home network operator with which the user 401 is signed on and registered.

[0009] In addition, the user 401, the dial-in network 403 and the home network 404 each have a central processing unit with a memory, for example a server (central computing unit), with which processing unit the procedure described below is monitored and controlled and on which memory data is stored.

[0010] The dial-in network 403 and the home network 404 are connected to one another via a data line over which digital data can be transmitted. The user 401 and the dial-in network 403 are connected to one another via any desired transmission medium for the transmission of digital data.

[0011] During a communication, the user 401 dials 410 into the dial-in network 403. At the start of the communication, checking of both the authenticity of the user 401 and the authenticity of the provider 402 is carried out.

[0012] To do this, the dial-in network 403 requests 411 what is referred to as authentication data from the home network 404, with which data the authenticity of the user 401 and of the provider 402 can be checked.

[0013] The authentication data which is obtained from the home network 404 comprises a random number and a sequential number of the provider 402. The sequential number of the provider 402 is obtained in such a way that a counter of the provider 402 increases the

sequential number of the provider 402 by the value 1 at each attempt at communication between the user 401 and the provider 402.

[0014] It is to be noted that the random number and the sequential number of the provider 402 only constitute part of the authentication data and are not to be understood as comprehensive. Further authentication data is known from [(1)]the 3G reference.

[0015] The home network 404 transmits 412 the requested authentication data to the dial-in network 403. The dial-in network 403 processes the received authentication data in a suitable way 413, and transmits [414] the processed authentication data to the user 401.

[0016] The user 401 checks 415 the authenticity of the provider 402 using a dedicated sequential number, which is handled in a way corresponding to the sequential number of the provider 402, and using the sequential number of the provider 402.

[0017] The procedure during the checking of the authenticity of the provider 402 is described in [(1)]the 3G reference.

[0018] A result of the checking of the authenticity of provider 402, "authenticity of provider satisfactory" 416, "authenticity of provider satisfactory but sequential fault has occurred" 417 or "authenticity of provider not satisfactory" 418, is transmitted 419 from the user 401 to the provider 402.

[0019] In the case of the result "authenticity of provider satisfactory" 416, the dial-in network 403 checks 420 the authenticity of the user 401 as described in [(1)]the 3G reference.

[0020] In the case of the result "authenticity of provider not satisfactory" 418, the communication is interrupted and/or restarted 421.

[0021] In the case of the result "authenticity of provider satisfactory but a sequential fault has occurred" 417, resynchronization takes place in such a way that the home network 404 transmits 422 a resynchronization request to the user 401. The user responds with a resynchronization response in which resynchronization data is transmitted 423 to the home network 404. The sequential number of the provider 402 is changed 424 as a function of the

resynchronization response. The authenticity of the user 401 is then checked, as is known from [(1)]the 3G reference.

[0022] The procedure described has the disadvantage that during checking of the authenticity of a communication subscriber, in particular during the checking of the authenticity of a service provider, a large amount of data has to be transmitted between the communication subscribers.

SUMMARY OF THE INVENTION

[0023] [The]One aspect of the invention is thus based on [the problem of disclosing a method which is simplified and improved in comparison with]simplifying and improving the known method and the known arrangement, [and a]to yield a simplified and improved arrangement for checking the authenticity of a communication subscriber in a communications network. [The problem is solved by means of the methods and by means of the arrangements having the features in accordance with the independent patent claims.]

[0024] In the method for checking the authenticity of a first communication subscriber in a communications network, a first fault information item is formed in the first communication subscriber using a fault detection data item of the first communication subscriber and an information item relating to a random data item. In a second communication subscriber in the communications network, a second fault information item is formed using a fault detection data item of the first communication subscriber and the information relating to the random data item.

[0025] The authenticity of the first communication subscriber is checked using the first fault information item and the second fault information item.

[0026] In the arrangement for checking the authenticity of a first communication subscriber in a communications network, the first communication subscriber is set up in such a way that a first fault information item can be formed using a fault detection data item of the first communication subscriber and an information item relating to a random data item. In addition, the arrangement has a second communication subscriber in the communications network which is set up in such a way that a second fault information item can be formed using a fault detection data item of the second communication subscriber and the information relating to the random data item. The

authenticity of the first communication subscriber can be checked using the first fault information item and the second fault information item.

[0027] The checking of the authenticity of a communication subscriber in a communications network is to be understood as meaning method steps which are carried out in the wider sense with checking of the authorization of a communication subscriber for access to a communications network or participation in communication in a communications network.

[0028] This thus encompasses both method steps which are carried out within the scope of the checking of the authorization of a communication subscriber for access to a communications network and such method steps which are carried out within the scope of the processing or the administration of data which is used in the checking. [Preferred developments of the invention are given in the dependent claims.]

[0029] The developments described below relate to the method and to the arrangement.

[0030] The [invention and the] development described below can be implemented either using software or hardware, for example using a specific electrical circuit.

[0031] In one refinement, the first communication subscriber is a service provider and/or the second communication subscriber is a service user in the communications network.

[0032] A sequential number is preferably used as the fault detection data item.

[0033] In one refinement, the information relating to the random data item is a random number.

[0034] In one development, the checking of the authenticity is simplified by determining a difference between the fault detection data item of the first communication subscriber and the fault detection data item of the second communication subscriber.

[0035] In one refinement, the checking of the authenticity is further improved with respect to the security of the communications network by limiting the difference.

[0036] One development is preferably used within the scope of a mobile phone system. In the mobile phone system, the service user is implemented as a mobile phone and/or the service provider is implemented as a mobile phone network operator.

BRIEF DESCRIPTION OF THE DRAWINGS

[0037] [An exemplary embodiment of the invention which is explained in more detail below is illustrated in the figures, in which figures]These and other objects and advantages of the present invention will become more apparent and more readily appreciated from the following description of the preferred embodiments, taken in conjunction with the accompanying drawings of which:

[Figure]Fig. 1 shows a mobile phone system;

[Figure]Fig. 2 shows an outline in which checking of the authenticity of a communication subscriber is illustrated symbolically;

[Figure]Fig. 3 shows a flowchart in which individual method steps are illustrated during checking of the authenticity of a service provider in a communications network; and

[Figure]Fig. 4 shows an outline in which checking of the authenticity of a communication subscriber in accordance with the 3G TS 33.102 Version 3.0.0 Standard is illustrated symbolically.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0038] Reference will now be made in detail to the preferred embodiments of the present invention, examples of which are illustrated in the accompanying drawings, wherein like reference numerals refer to like elements throughout.

Exemplary embodiment: mobile phone system

[0039] A mobile phone system 100 is illustrated in Fig. 1. The mobile phone system 100 comprises a mobile phone 101, a local dial-in network 102 with a dial-in network operator 103 and a home network 104 with a home network operator 105.

[0040] The mobile phone 101 is signed on and registered in the home network 104.

[0041] In addition, the mobile phone 101, the dial-in network 102 and the home network 104 each have a central processing unit 106, 107, 108 with a memory 109, 110, 111, with which processing units 106, 107, 108 the procedure described below is monitored and controlled, and on which memories 109, 110, 111 data is stored.

[0042] The dial-in network 102 and the home network 104 are connected to one another via a data line 112 via which digital data can be transmitted. The mobile phone 101 and the dial-in network 102 are connected to one another via any desired transmission medium 113 for transmitting digital data.

[0043] The procedure during the checking of the authenticity of the mobile phone 101 and the procedure during the checking of the authenticity of the home network 104 and/or of the home network operator 105 are illustrated symbolically in Fig. 2, and parts thereof will be explained below briefly.

[0044] The transmission of data in Fig. 2 is illustrated in each case by an arrow. A direction of an arrow characterizes a transmission direction during a data transmission.

[0045] The procedure which is described below and illustrated symbolically in Fig. 2 is based on what is referred to as a 3G TS 33.102 Version 3.0.0 Standard, which describes a security architecture of a mobile phone system and is described in [(1)]the 3G reference.

[0046] During a communication, the mobile phone 201 dials 210 into the dial-in network 203. At the start of the communication, checking both of the authenticity of the mobile phone 201 and of the authenticity of the home network 204 and/or of the home network operator takes place.

[0047] To do this, the dial-in network 203 requests 211 authentication data from the home network 204, with which authentication data the authenticity of the user 201 and of the home network 204 and/or of the home network operator can be checked.

[0048] The authentication data which is determined by the home network 204 comprises a random number and a sequential number of the home network 204 (cf. Fig. 3 step 310). The sequential number of the home network 204 is determined in such a way that a counter of the home network 204 increases the sequential number of the home network 204 by the value 1 at each attempt at communication between the mobile phone 201 and the home network 204.

[0049] It is to be noted that the random number and the sequential number of the home network 204 only constitute part of the authentication data and are not to be understood as comprehensive. Further authentication data is specified in [(1)]the 3G reference.

[0050] The home network 204 transmits 212 the requested authentication data to the dial-in network 203. The dial-in network 203 processes the received authentication data in a suitable way 213 and transmits [214] the processed authentication data to the mobile phone 201.

[0051] The mobile phone 201 checks 215 the authenticity of the home network 204 using a dedicated sequential number which is handled in a way corresponding to the sequential number of the home network 204, and using the sequential number of the home network 204. In a way corresponding to the home network 204, the mobile phone 201 also has a counter.

[0052] The procedure during the checking of the authenticity of the home network 204 is described in [(1)]the 3G reference. Method steps which differ therefrom are described below.

[0053] What is referred to as overflow checking of the counter of the mobile phone 201 is carried out within the scope of the checking of the authenticity of the home network 203. This overflow checking prevents overflowing of an acceptable numerical range of the counter of the mobile phone 201.

[0054] In the overflow checking, the following conditions are tested:

1) sequential number of the home network 204 > sequential number of the mobile phone 201;

2) sequential number of the home network 204 – sequential number of the mobile phone 201 < - predefinable deviation (1,000,000);

the following applying for the predefined deviation:

- predefinable deviation is sufficiently large in order to ensure, during normal or fault-free communications operation:

that the sequential number of the home network 204 – sequential number of the mobile phone 201 is not > predefinable deviation;

- the maximum permissable sequential number of the mobile phone 201/predefinable deviation is sufficiently large in order to ensure that the maximum permissible sequential number of the mobile phone 201 is not reached during operation.

[0055] The result of the checking of the authenticity of the home network 204, "authenticity satisfactory" 216, "authenticity satisfactory but a sequential fault has occurred" 217 or

"authenticity not satisfactory" 218 is transmitted [419]219 to the home network 204 from the mobile phone 201.

[0056] In the case of the result "authenticity satisfactory" 216, the dial-in network 203 checks 220 the authenticity of the mobile phone 201, as described in [(1)]3G reference.

[0057] In the case of the result "authenticity not satisfactory" 218, the communication is interrupted or restarted 221.

[0058] In the case of the result "authenticity satisfactory but a sequential fault has occurred" 217, resynchronization 222 takes place. Resynchronization is to be understood as a change of the sequential number of the home network 204.

[0059] For this purpose, the mobile phone 201 transmits 222 resynchronization data to the dial-in network 203.

[0060] The resynchronization data comprises the same random number which was transmitted within the scope of the authentication data, and the sequential number of the mobile phone 201 (cf. Fig. 3 step 320).

[0061] The dial-in network 203 processes the resynchronization data in a suitable way and transmits the processed resynchronization data to the home network 204.

[0062] The home network 204 checks the sequential number of the mobile phone 201 and the sequential number of the home network 204 using the processed resynchronization data, and if appropriate changes 223 the sequential number of the home network 204 (cf. Fig. 3 step 330).

[0063] The home network 204 subsequently transmits new authentication data, which if appropriate comprises the changed sequential number of the home network 204, to the dial-in network 203.

[0064] In order to illustrate the described procedure, important steps 300 of the procedure are illustrated in Fig. 3.

[0065] Fig. 3 shows a first step 310 within the scope of which the authentication data (first fault information) is determined.

[0066] The resynchronization data (second fault information) is determined within the scope of a second step 320.

[0067] The sequential number of the mobile phone and the sequential number of the home network are checked within the scope of a third step 330, using the resynchronization data.

[0068] An alternative of the first exemplary embodiment is described below.

[0069] In the alternative exemplary embodiment, a method is implemented in which the home network is made more reliable with respect to a data loss in the event of a system crash.

[0070] For this purpose, the current sequential number of the home network is stored in the memory of the home network, in each case at a predefinable time interval. A sequential number of the home network which has been lost during a system crash of the home network is restored in such a way that a predefinable additional value is added to the value of the stored sequential number. The predefinable additional value is dimensioned in such a way that exceeding of the sum of the sequential number of the mobile phone and the predefinable deviation is not exceeded.

[0071] In the alternative exemplary embodiment, the predefinable additional value is determined in such a way that an average number of authentication attempts on one day by the home network, which number is determined during operation of the communications network, is multiplied by a factor with the value 10.

[0072] The invention has been described in detail with particular reference to preferred embodiments thereof and examples, but it will be understood that variations and modifications can be effected within the spirit and scope of the invention. [The following publication is cited in this document: (1) 3G TS 33.102 Version 3.0.0 Draft Standard, 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Security Architecture, 05/1999.]

4/PRTS

Description

Method and arrangement for checking the authenticity of a first communication subscriber in a communications network

The invention relates to a method and an arrangement for checking the authenticity of a first communication subscriber in a communications network.

In a communications network, data is generally transmitted between communication subscribers, for example a service provider and a service user. In order to protect a communications network against penetration of an unauthorized communication subscriber into the communications network, the authenticity of each communication subscriber is generally checked.

Document [1] discloses a method and an arrangement for checking the authenticity of a communication subscriber, in particular of a service provider or of a service user in a communications network.

The method known from document [1] and the corresponding arrangement are based on what is referred to as 3G TS 33.102 Version 3.0.0 Draft Standard, which describes a security architecture of a mobile phone system.

In Fig. 4, the procedure during the checking of the authenticity of a communication subcriber, such as is known from the document [1] is illustrated symbolically and parts thereof will be explained below briefly.

A transmission of data is illustrated in Fig. 4 by an arrow in each case. A direction of an arrow characterizes a transmission direction during a data transmission.

Fig. 4 shows a mobile phone system 400, comprising a user 401 of a communication service, for example a mobile phone, and a provider 402 of a communication service. The provider 402 comprises a dial-in network 403 with a dial-in network operator from which the user 401 locally requests a communication service, and a home

network 404 with a home network operator with which the user 401 is signed on and registered.

In addition, the user 401, the dial-in network 403 and the home network 404 each have a central processing unit with a memory, for example a server (central computing unit), with which processing unit the procedure described below is monitored and controlled and on which memory data is stored.

The dial-in network 403 and the home network 404 are connected to one another via a data line over which digital data can be transmitted. The user 401 and the dial-in network 403 are connected to one another via any desired transmission medium for the transmission of digital data.

During a communication, the user 401 dials 410 into the dial-in network 403. At the start of the communication, checking of both the authenticity of the user 401 and the authenticity of the provider 402 is carried out.

To do this, the dial-in network 403 requests 411 what is referred to as authentication data from the home network 404, with which data the authenticity of the user 401 and of the provider 402 can be checked.

The authentication data which is obtained from the home network 404 comprises a random number and a sequential number of the provider 402. The sequential number of

the provider 402 is obtained in such a way that a counter of the provider 402 increases the sequential number of the provider 402 by the value 1 at each attempt at communication between the user

401 and the provider 402.

It is to be noted that the random number and the sequential number of the provider 402 only constitute part of the authentication data and are not to be understood as comprehensive. Further authentication data is known from [1].

The home network 404 transmits 412 the requested authentication data to the dial-in network 403. The dial-in network 403 processes the received authentication data in a suitable way 413, and transmits 414 the processed authentication data to the user 401.

The user 401 checks 415 the authenticity of the provider 402 using a dedicated sequential number, which is handled in a way corresponding to the sequential number of the provider 402, and using the sequential number of the provider 402.

The procedure during the checking of the authenticity of the provider 402 is described in [1].

A result of the checking of the authenticity of provider 402, "authenticity of provider satisfactory" 416, "authenticity of provider satisfactory but sequential fault has occurred" 417 or "authenticity of provider not satisfactory" 418, is transmitted 419 from the user 401 to the provider 402.

In the case of the result "authenticity of provider satisfactory" 416, the dial-in network 403 checks 420 the authenticity of the user 401 as described in [1].

In the case of the result "authenticity of provider not satisfactory" 418, the communication is interrupted and/or restarted 421.

In the case of the result "authenticity of provider satisfactory but a sequential fault has occurred" 417, resynchronization takes place in such a way that the home network 404 transmits 422 a resynchronization request to the user 401. The user responds with a resynchronization response in which resynchronization data is transmitted 423 to the home network 404. The sequential number of the provider 402 is changed 424 as a function of the resynchronization response. The authenticity of the user 401 is then checked, as is known from [1].

The procedure described has the disadvantage that during checking of the authenticity of a communication subscriber, in particular during the checking of the authenticity of a service provider, a large amount of data has to be transmitted between the communication subscribers.

The invention is thus based on the problem of disclosing a method which is simplified and improved in comparison with the known method and the known arrangement, and a simplified and improved arrangement for checking the authenticity of a communication subscriber in a communications network.

The problem is solved by means of the methods and by means of the arrangements having the features in accordance with the independent patent claims.

In the method for checking the authenticity of a first communication subscriber in a communications network, a first fault information item is formed in the first communication subscriber using a fault detection data item of the first communication subscriber and an information item relating to a random data item. In a second communication subscriber in the communications network, a second fault information item is formed

using a fault detection data item of the first communication subscriber and the information relating to the random data

item.

The authenticity of the first communication subscriber is checked using the first fault information item and the second fault information item.

In the arrangement for checking the authenticity of a first communication subscriber in a communications network, the first communication subscriber is set up in such a way that a first fault information item can be formed using a fault detection data item of the first communication subscriber and an information item relating to a random data item. In addition, the arrangement has a second communication subscriber in the communications network which is set up in such a way that a second fault information item can be formed using a fault detection data item of the second communication subscriber and the information relating to the random data item. The authenticity of the first communication subscriber can be checked using the first fault information item and the second fault information item.

The checking of the authenticity of a communication subscriber in a communications network is to be understood as meaning method steps which are carried out in the wider sense with checking of the authorization of a communication subscriber for access to a communications network or participation in communication in a communications network.

This thus encompasses both method steps which are carried out within the scope of the checking of the authorization of a communication subscriber for access to a communications network and such method steps which are carried out within the scope of the processing or the administration of data which is used in the checking.

Preferred developments of the invention are given in the dependent claims.

The developments described below relate to the method and to the arrangement.

The invention and the development described below can be implemented either using software or hardware, for example using a specific electrical circuit.

In one refinement, the first communication subscriber is a service provider and/or the second communication subscriber is a service user in the communications network.

A sequential number is preferably used as the fault detection data item.

In one refinement, the information relating to the random data item is a random number.

In one development, the checking of the authenticity is simplified by determining a difference between the fault detection data item of the first communication subscriber and the fault detection data item of the second communication subscriber.

In one refinement, the checking of the authenticity is further improved with respect to the security of the communications network by limiting the difference.

One development is preferably used within the scope of a mobile phone system. In the mobile phone system, the service user is implemented as a mobile phone and/or the service provider is implemented as a mobile phone network operator.

An exemplary embodiment of the invention which is explained in more detail below is illustrated in the figures, in which figures:

Figure 1 shows a mobile phone system;

Figure 2 shows an outline in which checking of the authenticity of a communication subscriber is illustrated symbolically;

Figure 3 shows a flowchart in which individual method steps are illustrated during checking of the authenticity of a service provider in a communications network;

Figure 4 shows an outline in which checking of the authenticity of a communication subscriber in accordance with the 3G TS 33.102 Version 3.0.0 Standard is illustrated symbolically.

Exemplary embodiment: mobile phone system

A mobile phone system 100 is illustrated in Fig. 1. The mobile phone system 100 comprises a mobile phone 101, a local dial-in network 102 with a dial-in network operator 103 and a home network 104 with a home network operator 105.

The mobile phone 101 is signed on and registered in the home network 104.

In addition, the mobile phone 101, the dial-in network 102 and the home network 104 each have a central processing unit 106, 107, 108 with a memory 109, 110, 111, with which processing units 106, 107, 108 the procedure described below is monitored and controlled, and

on which memories 109, 110, 111 data is stored.

The dial-in network 102 and the home network 104 are connected to one another via a data line 112 via which digital data can be transmitted. The mobile phone 101 and the dial-in network 102 are connected to one another via any desired transmission medium 113 for transmitting digital data.

The procedure during the checking of the authenticity of the mobile phone 101 and the procedure during the checking of the authenticity of the home network 104 and/or of the home network operator 105 are illustrated symbolically in Fig. 2, and parts thereof will be explained below briefly.

The transmission of data in Fig. 2 is illustrated in each case by an arrow. A direction of an arrow characterizes a transmission direction during a data transmission.

The procedure which is described below and illustrated symbolically in Fig. 2 is based on what is referred to as a 3G TS 33.102 Version 3.0.0 Standard, which describes a security architecture of a mobile phone system and is described in [1].

During a communication, the mobile phone 201 dials 210 into the dial-in network 203. At the start of the communication, checking both of the authenticity of the mobile phone 201 and of the authenticity of the home network 204 and/or of the home network operator takes place.

To do this, the dial-in network 203 requests 211 authentication data from the home network 204, with which authentication data the authenticity of the user 201 and of the home network 204 and/or of the home network operator can be checked.

The authentication data which is determined by the home network 204 comprises a random number and a sequential number of the home network 204 (cf. Fig. 3 step 310). The sequential number of the home network 204 is determined in such a way that a counter of the home network 204 increases the sequential number of the home

network 204 by the value 1 at each attempt at communication between the mobile phone 201 and the home network 204.

It is to be noted that the random number and the sequential number of the home network 204 only constitute part of the authentication data and are not to be understood as comprehensive. Further authentication data is specified in [1].

The home network 204 transmits 212 the requested authentication data to the dial-in network 203. The dial-in network 203 processes the received authentication data in a suitable way 213 and transmits 214 the processed authentication data to the mobile phone 201.

The mobile phone 201 checks 215 the authenticity of the home network 204 using a dedicated sequential number which is handled in a way corresponding to the sequential number of the home network 204, and using the sequential number of the home network 204. In a way corresponding to the home network 204, the mobile phone 201 also has a counter.

The procedure during the checking of the authenticity of the home network 204 is described in [1]. Method steps which differ therefrom are described below.

What is referred to as overflow checking of the counter of the mobile phone 201 is carried out within the scope

of the checking of the authenticity of the home network 203. This overflow checking prevents overflowing of an acceptable numerical range of the counter of the mobile phone 201.

In the overflow checking, the following conditions are tested:

1) sequential number of the home network 204 > sequential number of the mobile phone 201;

2) sequential number of the home network 204 - sequential number of the mobile phone 201 < - predefinable deviation (1,000,000);

the following applying for the predefined deviation:

- predefinable deviation is sufficiently large in order to ensure, during normal or fault-free communications operation:

that the sequential number of the home network 204 - sequential number of the mobile phone 201 is not > predefinable deviation;

- the maximum permissable sequential number of the mobile phone 201/predefinable deviation is sufficiently large in order to ensure that the maximum permissible sequential number of the mobile phone 201 is not reached during operation.

The result of the checking of the authenticity of the home network 204, "authenticity satisfactory" 216, "authenticity satisfactory but a sequential fault has occurred" 217 or "authenticity not satisfactory" 218 is transmitted 419 to the home network 204 from the mobile phone 201.

In the case of the result "authenticity satisfactory" 216, the dial-in network 203 checks 220 the authenticity of the mobile phone 201, as described in [1].

In the case of the result "authenticity not satisfactory" 218, the communication is interrupted or restarted 221.

In the case of the result "authenticity satisfactory but a sequential fault has occurred" 217, resynchronization 222 takes place. Resynchronization is to be understood as a change of the sequential number of the home network 204.

For this purpose, the mobile phone 201 transmits 222 resynchronization data to the dial-in network 203.

The resynchronization data comprises the same random number which was transmitted within the scope of the authentication data, and the sequential number of the mobile phone 201 (cf. Fig. 3 step 320).

The dial-in network 203 processes the resynchronization data in a suitable way and transmits the processed resynchronization data to the home network 204.

The home network checks the sequential number of the mobile phone 201 and the sequential number of the home network 204 using the processed resynchronization data, and if appropriate changes 223 the sequential number of the home network 204 (cf. Fig. 3 step 330).

The home network 204 subsequently transmits new authentication data, which if appropriate comprises the changed sequential number of the home network 204, to the dial-in network 203.

In order to illustrate the described procedure, important steps 300 of the procedure are illustrated in Fig. 3.

Fig. 3 shows a first step 310 within the scope of which the authentication data (first fault information) is determined.

The resynchronization data (second fault information) is determined within the scope of a second step 320.

The sequential number of the mobile phone and the sequential number of the home network are checked within the scope of a third step 330, using the resynchronization data.

An alternative of the first exemplary embodiment is described below.

In the alternative exemplary embodiment, a method is implemented in which the home network is made more reliable with respect to a data loss in the event of a system crash.

For this purpose, the current sequential number of the home network is stored in the memory of the home network, in each case at a predefinable time interval. A sequential number of the home network which has been lost during a system crash of the home network is restored in such a way that a predefinable additional value is added to the value of the stored sequential number. The predefinable additional value is dimensioned in such a way that exceeding of the sum of the sequential number of the mobile phone and the predefinable deviation is not exceeded.

In the alternative exemplary embodiment, the predefinable additional value is determined in such a way that an average number of authentication attempts on one day by the home network, which number is determined during operation of the communications network, is multiplied by a factor with the value 10.

The following publication is cited in this document:

[1] 3G TS 33.102 Version 3.0.0 Draft Standard, 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Security Architecture, 05/1999.

Patent claims

1. A method for checking the authenticity of a first communication subscriber in a communications network,
   - in which a first fault information item is formed in the first communication subscriber using a fault detection data item of the service provider and an information item relating to a random data item;
   - in which a second fault information item is formed in a second communication subscriber in the communications network using a fault detection data item of the second communication subscriber and the information item relating to the random data item;
   - in which the authenticity of the first communication subscriber is checked using the first fault information item and the second fault information item.

2. The method as claimed in claim 1, in which a difference is determined between the fault detection data item of the first communication subscriber and the fault detection data item of the second communication subscriber.

3. The method as claimed in claim 2, in which the difference is limited.

4. The method as claimed in one of claims 1 to 3, used within the scope of a mobile phone system.

5. An arrangement for checking the authenticity of a first communication subscriber in a communications network,

- in which the first communication subscriber is set up in such a way that a first fault information item can be formed using a fault detection data item of the first communication subscriber and an information item relating to a random data item;

- in which a second communication subscriber is set up in the communications network in such a way that a second fault information item can be formed using a fault detection data item of the second communication subscriber and the information relating to the random data item;
- in which the authenticity of the first communication subscriber can be checked using the first fault information and the second fault information.

6. The arrangement as claimed in claim 5, in which the first communication subscriber is a service provider and/or the second communication subscriber is a service user in the communications network.

7. The arrangement as claimed in claim 5 or 6, in which a fault detection data item is a sequential number.

8. The arrangement as claimed in one of claims 5 to 7, in which the information relating to the random data item is a random number.

9. The arrangement as claimed in one of claims 5 to 8, in which the first communication subscriber is a service provider in the communications network and/or the second communication subscriber is a service user in the communications network.

10. The arrangement as claimed in claim 9, in which the service provider is a mobile phone operator and/or the service user is a mobile phone.

11. The arrangement as claimed in one of claims 5 to 10, used within the scope of a mobile phone system.

Abstract

Method and arrangement for checking the authenticity of a first communication subscriber in a communications network

In the method and the arrangement for checking the authenticity of a first communication subscriber in a communications network, a first fault information item is formed in the first communication subscriber using a fault detection data item of the first communication subscriber and an information item relating to a random data item. In a second communication subscriber in the communications network, a second fault information item is formed using a fault detection data item of the second communication subscriber and the information relating to the random data item. The authenticity of the first communication subscriber is checked using the first fault information and the second fault information.

Patent claims

1. A method for checking the authenticity of a first communication subscriber in a communications network,
   - in which a first fault information item is formed in the first communication subscriber using a fault detection data item of the first communication subscriber and an information item relating to a random data item which has been transmitted to the first communication subscriber by a second communication subscriber in the communications network;
   - in which the first fault information is transmitted to the second communication subscriber by the first communication subscriber,
   - in which a second fault information item is formed in the second communication subscriber using a fault detection data item of the second communication subscriber and the information item relating to the random data item;
   - in which the authenticity of the first communication subscriber is checked in the second communication subscriber using the first fault information item and the second fault information item.

2. The method as claimed in claim 1, in which a difference is determined between the fault detection data item of the first communication subscriber and the fault detection data item of the second communication subscriber.

3. The method as claimed in claim 2, in which the difference is limited.

4. The method as claimed in one of claims 1 to 3, used within the scope of a mobile phone system.

5. An arrangement for checking the authenticity of a first communication subscriber in a communications network,

- in which the first communication subscriber is set up in such a way that a first fault information item can be formed using a fault detection data item of the first communication subscriber and an information item relating to a random data item which has been transmitted to the first communication subscriber by a second communication subscriber in the communications network, and the first fault information item can be transmitted to the second communication subscriber;
- in which the second communication subscriber is set up in such a way that a second fault information item can be formed using a fault detection data item of the second communication subscriber and the information relating to the random data item, and the authenticity of the first communication subscriber can be checked using the first fault information and the second fault information.

6. The arrangement as claimed in claim 5, in which the first communication subscriber is a service provider and/or the second communication subscriber is a service user in the communications network.

7. The arrangement as claimed in claim 5 or 6, in which a fault detection data item is a sequential number.

8. The arrangement as claimed in one of claims 5 to 7, in which the information relating to the random data item is a random number.

9. The arrangement as claimed in one of claims 5 to 8, in which the first communication subscriber is a service provider in the communications network and/or the second communication subscriber is a service user in the communications network.

10. The arrangement as claimed in claim 9, in which the service provider is a mobile phone operator and/or the service user is a mobile phone.

11. The arrangement as claimed in one of claims 5 to 10, used within the scope of a mobile phone system.

Description

Method and arrangement for checking the authenticity of a first communication subscriber in a communications network

The invention relates to a method and an arrangement for checking the authenticity of a first communication subscriber in a communications network.

In a communications network, data is generally transmitted between communication subscribers, for example a service provider and a service user. In order to protect a communications network against penetration of an unauthorized communication subscriber into the communications network, the authenticity of each communication subscriber is generally checked.

Document [1] discloses a method and an arrangement for checking the authenticity of a communication subscriber, in particular of a service provider or of a service user in a communications network.

The method known from document [1] and the corresponding arrangement are based on what is referred to as 3G TS 33.102 Version 3.0.0 Draft Standard, which describes a security architecture of a mobile phone system.

In Fig. 4, the procedure during the checking of the authenticity of a communication subcriber, such as is known from the document [1] is illustrated symbolically and parts thereof will be explained below briefly.

A transmission of data is illustrated in Fig. 4 by an arrow in each case. A direction of an arrow characterizes a transmission direction during a data transmission.
Fig. 4 shows a mobile phone system 400, comprising a user 401 of a communication service, for example a mobile phone, and a provider 402 of a communication service. The provider 402 comprises a dial-in network 403 with a dial-in network operator from which the user 401 locally requests a communication service, and a home

network 404 with a home network operator with which the user 401 is signed on and registered.

In addition, the user 401, the dial-in network 403 and the home network 404 each have a central processing unit with a memory, for example a server (central computing unit), with which processing unit the procedure described below is monitored and controlled and on which memory data is stored.

The dial-in network 403 and the home network 404 are connected to one another via a data line over which digital data can be transmitted. The user 401 and the dial-in network 403 are connected to one another via any desired transmission medium for the transmission of digital data.

During a communication, the user 401 dials 410 into the dial-in network 403. At the start of the communication, checking of both the authenticity of the user 401 and the authenticity of the provider 402 is carried out.

To do this, the dial-in network 403 requests 411 what is referred to as authentication data from the home network 404, with which data the authenticity of the user 401 and of the provider 402 can be checked.

The authentication data which is obtained from the home network 404 comprises a random number and a sequential number of the provider 402. The sequential number of

the provider 402 is obtained in such a way that a counter of the provider 402 increases the sequential number of the provider 402 by the value 1 at each attempt at communication between the user

401 and the provider 402.

It is to be noted that the random number and the sequential number of the provider 402 only constitute part of the authentication data and are not to be understood as comprehensive. Further authentication data is known from [1].

The home network 404 transmits 412 the requested authentication data to the dial-in network 403. The dial-in network 403 processes the received authentication data in a suitable way 413, and transmits 414 the processed authentication data to the user 401.

The user 401 checks 415 the authenticity of the provider 402 using a dedicated sequential number, which is handled in a way corresponding to the sequential number of the provider 402, and using the sequential number of the provider 402.

The procedure during the checking of the authenticity of the provider 402 is described in [1].

A result of the checking of the authenticity of provider 402, "authenticity of provider satisfactory" 416, "authenticity of provider satisfactory but sequential fault has occurred" 417 or "authenticity of provider not satisfactory" 418, is transmitted 419 from the user 401 to the provider 402.

In the case of the result "authenticity of provider satisfactory" 416, the dial-in network 403 checks 420 the authenticity of the user 401 as described in [1].

In the case of the result "authenticity of provider not satisfactory" 418, the communication is interrupted and/or restarted 421.

In the case of the result "authenticity of provider satisfactory but a sequential fault has occurred" 417, resynchronization takes place in such a way that the home network 404 transmits 422 a resynchronization request to the user 401. The user responds with a resynchronization response in which resynchronization data is transmitted 423 to the home network 404. The sequential number of the provider 402 is changed 424 as a function of the resynchronization response. The authenticity of the user 401 is then checked, as is known from [1].

The procedure described has the disadvantage that during checking of the authenticity of a communication subscriber, in particular during the checking of the authenticity of a service provider, a large amount of data has to be transmitted between the communication subscribers.

The invention is thus based on the problem of disclosing a method which is simplified and improved in comparison with the known method and the known arrangement, and a simplified and improved arrangement for checking the authenticity of a communication subscriber in a communications network.

The problem is solved by means of the methods and by means of the arrangements having the features in accordance with the independent patent claims.

In the method for checking the authenticity of a first communication subscriber in a communications network, a first fault information item is formed in the first communication subscriber using a fault detection data item of the first communication subscriber and an information item relating to a random data item. In a second communication subscriber in the communications network, a second fault information item is formed

using a fault detection data item of the first communication subscriber and the information relating to the random data

item.

The authenticity of the first communication subscriber is checked using the first fault information item and the second fault information item.

In the arrangement for checking the authenticity of a first communication subscriber in a communications network, the first communication subscriber is set up in such a way that a first fault information item can be formed using a fault detection data item of the first communication subscriber and an information item relating to a random data item. In addition, the arrangement has a second communication subscriber in the communications network which is set up in such a way that a second fault information item can be formed using a fault detection data item of the second communication subscriber and the information relating to the random data item. The authenticity of the first communication subscriber can be checked using the first fault information item and the second fault information item.

The checking of the authenticity of a communication subscriber in a communications network is to be understood as meaning method steps which are carried out in the wider sense with checking of the authorization of a communication subscriber for access to a communications network or participation in communication in a communications network.

This thus encompasses both method steps which are carried out within the scope of the checking of the authorization of a communication subscriber for access to a communications network and such method steps which are carried out within the scope of the processing or the administration of data which is used in the checking.

Preferred developments of the invention are given in the dependent claims.

The developments described below relate to the method and to the arrangement.

The invention and the development described below can be implemented either using software or hardware, for example using a specific electrical circuit.

In one refinement, the first communication subscriber is a service provider and/or the second communication subscriber is a service user in the communications network.

A sequential number is preferably used as the fault detection data item.

In one refinement, the information relating to the random data item is a random number.

In one development, the checking of the authenticity is simplified by determining a difference between the fault detection data item of the first communication subscriber and the fault detection data item of the second communication subscriber.

In one refinement, the checking of the authenticity is further improved with respect to the security of the communications network by limiting the difference.

One development is preferably used within the scope of a mobile phone system. In the mobile phone system, the service user is implemented as a mobile phone and/or the service provider is implemented as a mobile phone network operator.

An exemplary embodiment of the invention which is explained in more detail below is illustrated in the figures, in which figures:

Figure 1 shows a mobile phone system;

Figure 2 shows an outline in which checking of the authenticity of a communication subscriber is illustrated symbolically;

Figure 3 shows a flowchart in which individual method steps are illustrated during checking of the authenticity of a service provider in a communications network;

Figure 4 shows an outline in which checking of the authenticity of a communication subscriber in accordance with the 3G TS 33.102 Version 3.0.0 Standard is illustrated symbolically.

Exemplary embodiment: mobile phone system

A mobile phone system 100 is illustrated in Fig. 1. The mobile phone system 100 comprises a mobile phone 101, a local dial-in network 102 with a dial-in network operator 103 and a home network 104 with a home network operator 105.

The mobile phone 101 is signed on and registered in the home network 104.

In addition, the mobile phone 101, the dial-in network 102 and the home network 104 each have a central processing unit 106, 107, 108 with a memory 109, 110, 111, with which processing units 106, 107, 108 the procedure described below is monitored and controlled, and

on which memories 109, 110, 111 data is stored.

The dial-in network 102 and the home network 104 are connected to one another via a data line 112 via which digital data can be transmitted. The mobile phone 101 and the dial-in network 102 are connected to one another via any desired transmission medium 113 for transmitting digital data.

The procedure during the checking of the authenticity of the mobile phone 101 and the procedure during the checking of the authenticity of the home network 104 and/or of the home network operator 105 are illustrated symbolically in Fig. 2, and parts thereof will be explained below briefly.

The transmission of data in Fig. 2 is illustrated in each case by an arrow. A direction of an arrow characterizes a transmission direction during a data transmission.

The procedure which is described below and illustrated symbolically in Fig. 2 is based on what is referred to as a 3G TS 33.102 Version 3.0.0 Standard, which describes a security architecture of a mobile phone system and is described in [1].

During a communication, the mobile phone 201 dials 210 into the dial-in network 203. At the start of the communication, checking both of the authenticity of the mobile phone 201 and of the authenticity of the home network 204 and/or of the home network operator takes place.

To do this, the dial-in network 203 requests 211 authentication data from the home network 204, with which authentication data the authenticity of the user 201 and of the home network 204 and/or of the home network operator can be checked.

The authentication data which is determined by the home network 204 comprises a random number and a sequential number of the home network 204 (cf. Fig. 3 step 310). The sequential number of the home network 204 is determined in such a way that a counter of the home network 204 increases the sequential number of the home

network 204 by the value 1 at each attempt at communication between the mobile phone 201 and the home network 204.

It is to be noted that the random number and the sequential number of the home network 204 only constitute part of the authentication data and are not to be understood as comprehensive. Further authentication data is specified in [1].

The home network 204 transmits 212 the requested authentication data to the dial-in network 203. The dial-in network 203 processes the received authentication data in a suitable way 213 and transmits 214 the processed authentication data to the mobile phone 201.

The mobile phone 201 checks 215 the authenticity of the home network 204 using a dedicated sequential number which is handled in a way corresponding to the sequential number of the home network 204, and using the sequential number of the home network 204. In a way corresponding to the home network 204, the mobile phone 201 also has a counter.

The procedure during the checking of the authenticity of the home network 204 is described in [1]. Method steps which differ therefrom are described below.

What is referred to as overflow checking of the counter of the mobile phone 201 is carried out within the scope

of the checking of the authenticity of the home network 203. This overflow checking prevents overflowing of an acceptable numerical range of the counter of the mobile phone 201.

In the overflow checking, the following conditions are tested:

1) sequential number of the home network 204 > sequential number of the mobile phone 201;

2) sequential number of the home network 204 - sequential number of the mobile phone 201 < - predefinable deviation (1,000,000);

the following applying for the predefined deviation:

- predefinable deviation is sufficiently large in order to ensure, during normal or fault-free communications operation:

that the sequential number of the home network 204 - sequential number of the mobile phone 201 is not > predefinable deviation;

- the maximum permissable sequential number of the mobile phone 201/predefinable deviation is sufficiently large in order to ensure that the maximum permissible sequential number of the mobile phone 201 is not reached during operation.

The result of the checking of the authenticity of the home network 204, "authenticity satisfactory" 216, "authenticity satisfactory but a sequential fault has occurred" 217 or "authenticity not satisfactory" 218 is transmitted 419 to the home network 204 from the mobile phone 201.

In the case of the result "authenticity satisfactory" 216, the dial-in network 203 checks 220 the authenticity of the mobile phone 201, as described in [1].

In the case of the result "authenticity not satisfactory" 218, the communication is interrupted or restarted 221.

In the case of the result "authenticity satisfactory but a sequential fault has occurred" 217, resynchronization 222 takes place. Resynchronization is to be understood as a change of the sequential number of the home network 204.

For this purpose, the mobile phone 201 transmits 222 resynchronization data to the dial-in network 203.

The resynchronization data comprises the same random number which was transmitted within the scope of the authentication data, and the sequential number of the mobile phone 201 (cf. Fig. 3 step 320).

The dial-in network 203 processes the resynchronization data in a suitable way and transmits the processed resynchronization data to the home network 204.

The home network checks the sequential number of the mobile phone 201 and the sequential number of the home network 204 using the processed resynchronization data, and if appropriate changes 223 the sequential number of the home network 204 (cf. Fig. 3 step 330).

The home network 204 subsequently transmits new authentication data, which if appropriate comprises the changed sequential number of the home network 204, to the dial-in network 203.

In order to illustrate the described procedure, important steps 300 of the procedure are illustrated in Fig. 3.

Fig. 3 shows a first step 310 within the scope of which the authentication data (first fault information) is determined.

The resynchronization data (second fault information) is determined within the scope of a second step 320.

The sequential number of the mobile phone and the sequential number of the home network are checked within the scope of a third step 330, using the resynchronization data.

An alternative of the first exemplary embodiment is described below.

In the alternative exemplary embodiment, a method is implemented in which the home network is made more reliable with respect to a data loss in the event of a system crash.

For this purpose, the current sequential number of the home network is stored in the memory of the home network, in each case at a predefinable time interval. A sequential number of the home network which has been lost during a system crash of the home network is restored in such a way that a predefinable additional value is added to the value of the stored sequential number. The predefinable additional value is dimensioned in such a way that exceeding of the sum of the sequential number of the mobile phone and the predefinable deviation is not exceeded.

In the alternative exemplary embodiment, the predefinable additional value is determined in such a way that an average number of authentication attempts on one day by the home network, which number is determined during operation of the communications network, is multiplied by a factor with the value 10.

The following publication is cited in this document:

[1] 3G TS 33.102 Version 3.0.0 Draft Standard, 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Security Architecture, 05/1999.

Patent claims

1. A method for checking the authenticity of a first communication subscriber in a communications network,
   - in which a first fault information item is formed in the first communication subscriber using a fault detection data item of the first communication subscriber and an information item relating to a random data item which has been transmitted to the first communication subscriber by a second communication subscriber in the communications network;
   - in which the first fault information is transmitted to the second communication subscriber by the first communication subscriber,
   - in which a second fault information item is formed in the second communication subscriber using a fault detection data item of the second communication subscriber and the information item relating to the random data item;
   - in which the authenticity of the first communication subscriber is checked in the second communication subscriber using the first fault information item and the second fault information item.

2. The method as claimed in claim 1, in which a difference is determined between the fault detection data item of the first communication subscriber and the fault detection data item of the second communication subscriber.

3. The method as claimed in claim 2, in which the difference is limited.

4. The method as claimed in one of claims 1 to 3, used within the scope of a mobile phone system.

5. An arrangement for checking the authenticity of a first communication subscriber in a communications network,

- in which the first communication subscriber is set up in such a way that a first fault information item can be formed using a fault detection data item of the first communication subscriber and an information item relating to a random data item which has been transmitted to the first communication subscriber by a second communication subscriber in the communications network, and the first fault information item can be transmitted to the second communication subscriber;
- in which the second communication subscriber is set up in such a way that a second fault information item can be formed using a fault detection data item of the second communication subscriber and the information relating to the random data item, and the authenticity of the first communication subscriber can be checked using the first fault information and the second fault information.

6. The arrangement as claimed in claim 5, in which the first communication subscriber is a service provider and/or the second communication subscriber is a service user in the communications network.

7. The arrangement as claimed in claim 5 or 6, in which a fault detection data item is a sequential number.

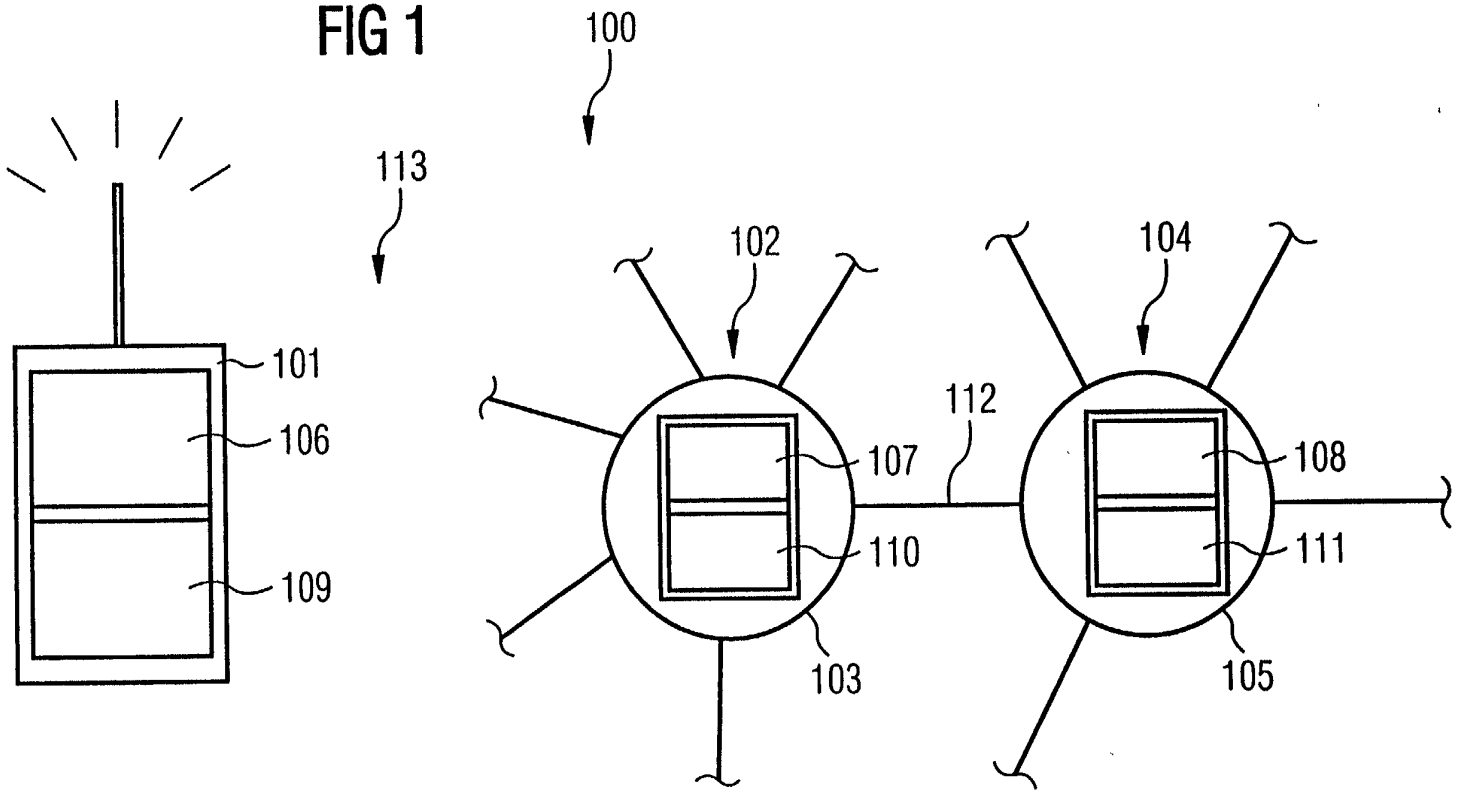
8. The arrangement as claimed in one of claims 5 to 7, in which the information relating to the random data item is a random number.

9. The arrangement as claimed in one of claims 5 to 8, in which the first communication subscriber is a service provider in the communications network and/or the second communication subscriber is a service user in the communications network.

10. The arrangement as claimed in claim 9, in which the service provider is a mobile phone operator and/or the service user is a mobile phone.

11. The arrangement as claimed in one of claims 5 to 10, used within the scope of a mobile phone system.

FIG 1



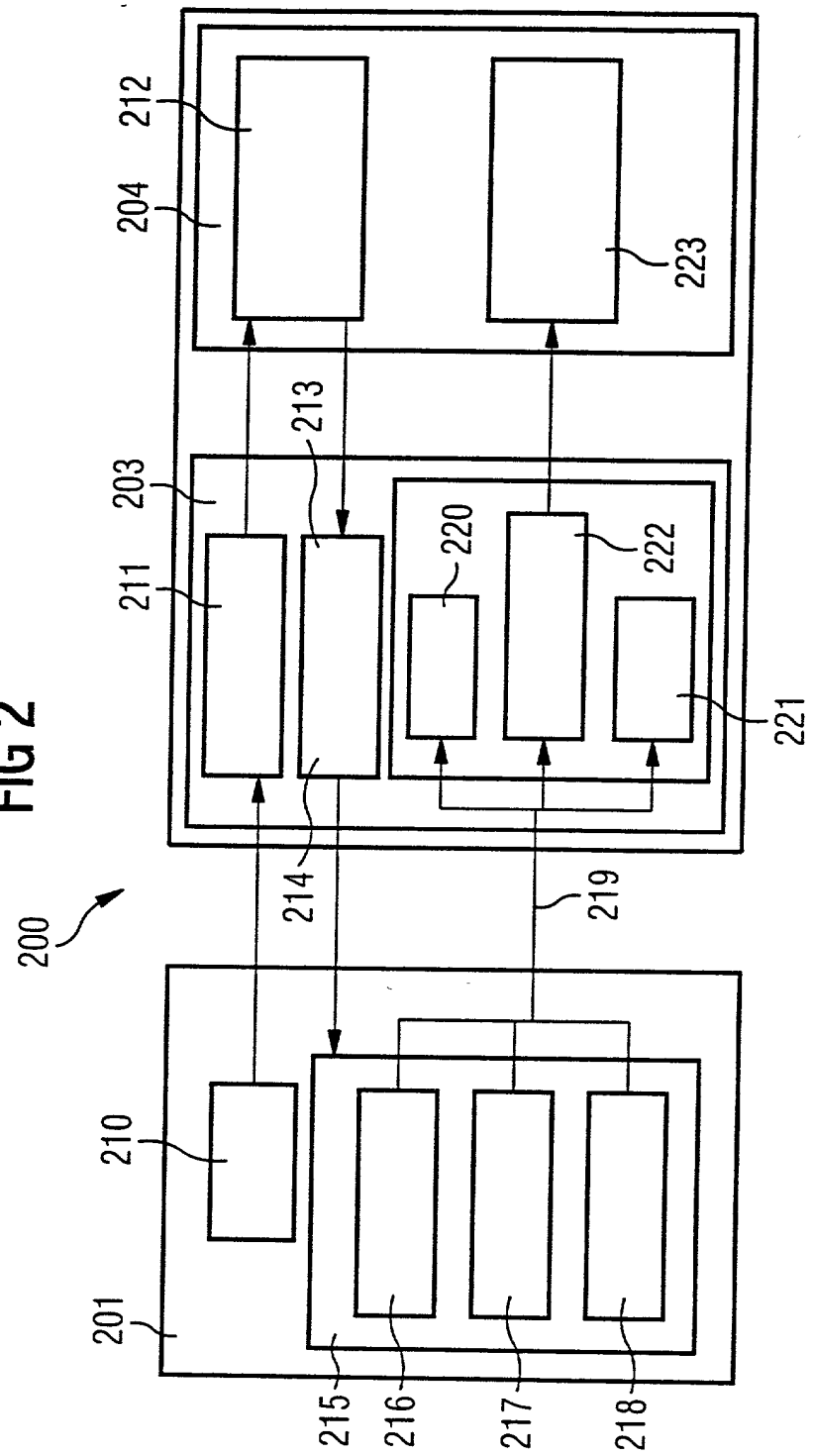
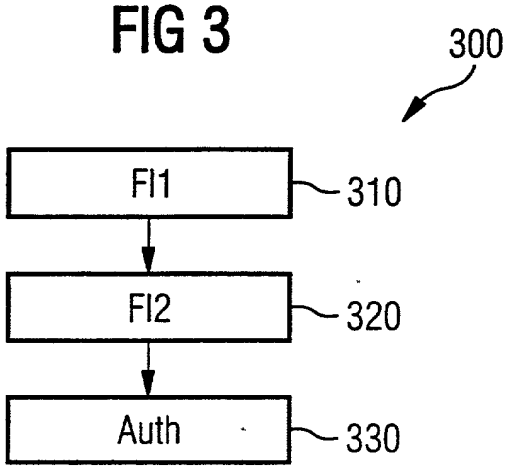

200
201
203
204
210
211
212
213
214
215
216
217
218
219
220
221
222
223

FIG 2

FIG 3



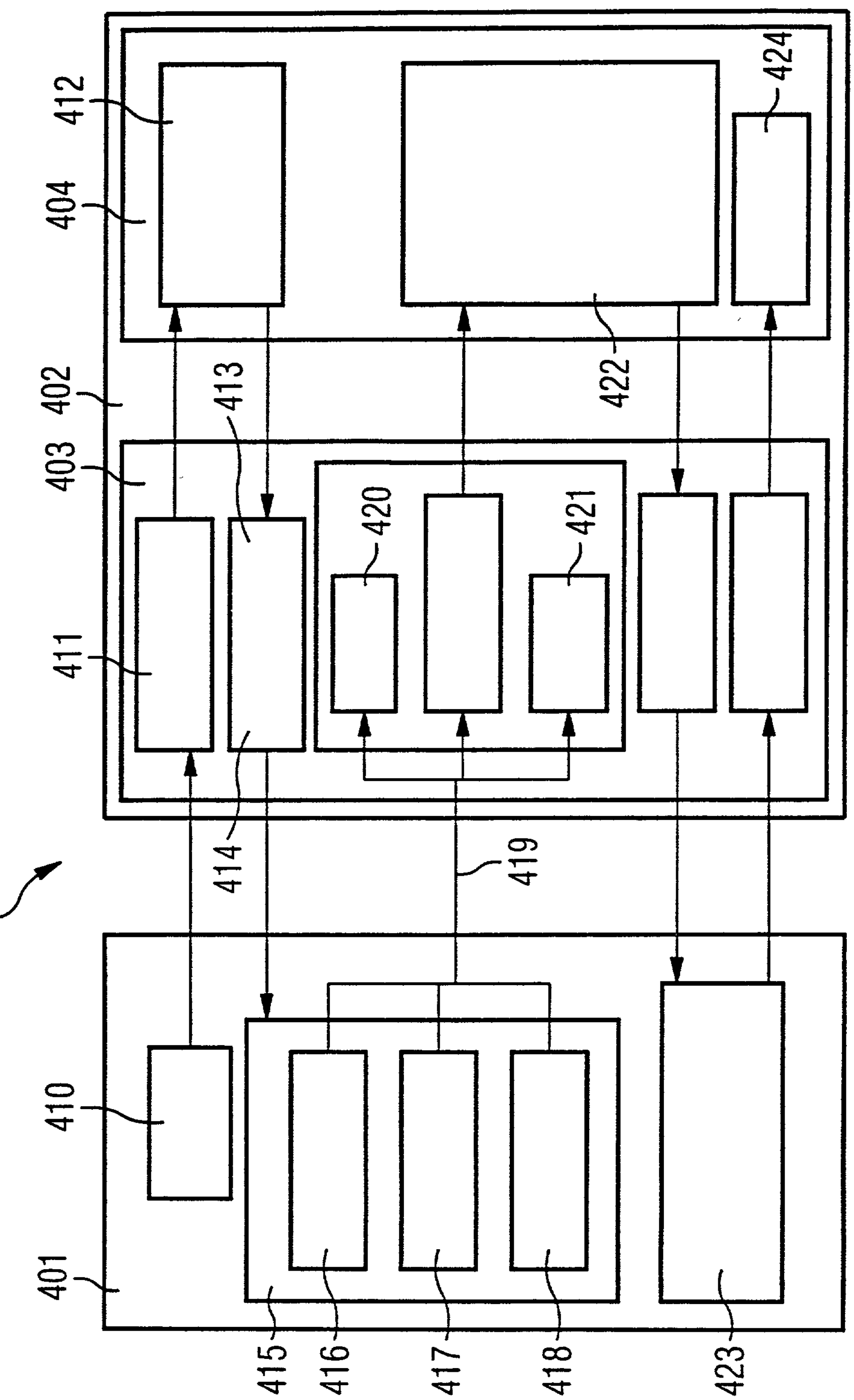

400
401
402
403
404
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424

FIG 4

Declaration and Power of Attorney For Patent Application
Erklärung Für Patentanmeldungen Mit Vollmacht
German Language Declaration

Als nachstehend benannter Erfinder erkläre ich hiermit an Eides Statt:

As a below named inventor, I hereby declare that:

dass mein Wohnsitz, meine Postanschrift, und meine Staatsangehörigkeit den im Nachstehenden nach meinem Namen aufgeführten Angaben entsprechen,

My residence, post office address and citizenship are as stated below next to my name,

dass ich, nach bestem Wissen der ursprüngliche, erste und alleinige Erfinder (falls nachstehend nur ein Name angegeben ist) oder ein ursprünglicher, erster und Miterfinder (falls nachstehend mehrere Namen aufgeführt sind) des Gegenstandes bin, für den dieser Antrag gestellt wird und für den ein Patent beantragt wird für die Erfindung mit dem Titel:

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

Verfahren und Anordnung zur Überprüfung einer Authentizität eines ersten Kommunikationsteilnehmers in einem Kommunikationsnetz

Method and system for verifying the authenticity of a first communication participants in a communication network

deren Beschreibung

(zutreffendes ankreuzen)
☐ hier beigefügt ist.
☒ am 31.05.2000 als PCT internationale Anmeldung PCT Anmeldungsnummer PCT/DE00/01788 eingereicht wurde und am _____ abgeändert wurde (falls tatsächlich abgeändert).

the specification of which

(check one)
☐ is attached hereto.
☒ was filed on 31.05.2000 as PCT international application PCT Application No. PCT/DE00/01788 and was amended on _____ (if applicable)

Ich bestätige hiermit, dass ich den Inhalt der obigen Patentanmeldung einschliesslich der Ansprüche durchgesehen und verstanden habe, die eventuell durch einen Zusatzantrag wie oben erwähnt abgeändert wurde.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims as amended by any amendment referred to above.

Ich erkenne meine Pflicht zur Offenbarung irgendwelcher Informationen, die für die Prüfung der vorliegenden Anmeldung in Einklang mit Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) von Wichtigkeit sind, an.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

Ich beanspruche hiermit ausländische Prioritätsvorteile gemäss Abschnitt 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 119 aller unten angegebenen Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde, und habe auch alle Auslandsanmeldungen für ein Patent oder eine Erfindersurkunde nachstehend gekennzeichnet, die ein Anmeldedatum haben, das vor dem Anmeldedatum der Anmeldung liegt, für die Priorität beansprucht wird.

I hereby claim foreign priority benefits under Title 35, United States Code, §119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed.

German Language Declaration

Prior foreign appplications
Priorität beansprucht

Priority Claimed

19927271.9 (Number) (Nummer)	DE (Country) (Land)	15.06.1999 (Day Month Year Filed) (Tag Monat Jahr eingereicht)	☒ Yes Ja	☐ No Nein
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	☐ Yes Ja	☐ No Nein
(Number) (Nummer)	(Country) (Land)	(Day Month Year Filed) (Tag Monat Jahr eingereicht)	☐ Yes Ja	☐ No Nein

Ich beanspruche hiermit gemäss Absatz 35 der Zivilprozessordnung der Vereinigten Staaten, Paragraph 120, den Vorzug aller unten aufgeführten Anmeldungen und falls der Gegenstand aus jedem Anspruch dieser Anmeldung nicht in einer früheren amerikanischen Patentanmeldung laut dem ersten Paragraphen des Absatzes 35 der Zivilprozeßordnung der Vereinigten Staaten, Paragraph 122 offenbart ist, erkenne ich gemass Absatz 37, Bundesgesetzbuch, Paragraph 1.56(a) meine Pflicht zur Offenbarung von Informationen an, die zwischen dem Anmeldedatum der früheren Anmeldung und dem nationalen oder PCT internationalen Anmeldedatum dieser Anmeldung bekannt geworden sind.

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §122, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application.

PCT/DE00/01788 (Application Serial No.) (Anmeldeserlennummer)	31.05.2000 (Filing Date D. M. Y) (Anmeldedatum T. M. J)	anhängig (Status) (patentiert, anhängig, aufgegeben)	pending (Status) (patented, pending, abandoned)
(Application Serial No.) (Anmeldeserlennummer)	(Filing Date D,M,Y) (Anmeldedatum T, M, J)	(Status) (patentiert, anhängig, aufgeben)	(Status) (patented, pending, abandoned)

Ich erkläre hiermit, dass alle von mir in der vorliegenden Erklärung gemachten Angaben nach meinem besten Wissen und Gewissen der vollen Wahrheit entsprechen, und dass ich diese eidesstattliche Erklärung in Kenntnis dessen abgebe, dass wissentlich und vorsätzlich falsche Angaben gemäss Paragraph 1001, Absatz 18 der Zivilprozessordnung der Vereinigten Staaten von Amerika mit Geldstrafe belegt und/oder Gefangnis bestraft werden koennen, und dass derartig wissentlich und vorsätzlich falsche Angaben die Gültigkeit der vorliegenden Patentanmeldung oder eines darauf erteilten Patentes gefährden können.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

German Language Declaration

VERTRETUNGSVOLLMACHT: Als benannter Erfinder beauftrage ich hiermit den nachstehend benannten Patentanwalt (oder die nachstehend benannten Patentanwälte) und/oder Patent-Agenten mit der Verfolgung der vorliegenden Patentanmeldung sowie mit der Abwicklung aller damit verbundenen Geschäfte vor dem Patent- und Warenzeichenamt: *(Name und Registrationsnummer anführen)*

POWER OF ATTORNEY. As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

And I hereby appoint

Customer No. 21171

Telefongespräche bitte richten an: *(Name und Telefonnummer)*

Direct Telephone Calls to: *(name and telephone number)*

Ext. _____

Postanschrift:

Send Correspondence to:

Staas & Halsey LLP
700 Eleventh Street NW, Suite 500 20001 Washington, DC
Telephone: (001) 202 434 1500 and Facsimile (001) 202 434 1501
or
Customer No. 21171

Voller Name des einzigen oder ursprünglichen Erfinders:	Full name of sole or first inventor:
Dr. JORGE CUELLAR	Dr. JORGE CUELLAR
Unterschrift des Erfinders: Jorge R Cuellar — Datum: 11-03-02	Inventor's signature: Jorge R Cuellar — Date: 11-03-02
Wohnsitz: BAIERBRUNN, DEUTSCHLAND (DE)	Residence: BAIERBRUNN, GERMANY
Staatsangehörigkeit: DE	Citizenship: DE
Postanschrift: HOELLRIEGELSKREUTHER WEG 14 82065 BAIERBRUNN	Post Office Address: HOELLRIEGELSKREUTHER WEG 14 82065 BAIERBRUNN
Voller Name des zweiten Miterfinders (falls zutreffend): Dr. GUENTHER HORN	Full name of second joint inventor, if any: Dr. GUENTHER HORN
Unterschrift des Erfinders: Günther Horn — Datum: 11-03-02	Second inventor's signature: Günther Horn — Date: 11-03-02
Wohnsitz: MUENCHEN, DEUTSCHLAND (DE)	Residence: MUENCHEN, GERMANY
Staatsangehörigkeit: DE	Citizenship: DE
Postanschrift: EDUARD-SCHMID-STR. 16 81541 MUENCHEN	Post Office Address: EDUARD-SCHMID-STR. 16 81541 MUENCHEN

(Bitte entsprechende Informationen und Unterschriften im Falle von dritten und weiteren Miterfindern angeben).

(Supply similar information and signature for third and subsequent joint inventors).